CLAIMS

What is claimed is:

1. A security system for controlling access to a trusted computer network by a client computer, comprising:

a bastion host that controls access to said trusted computer network;

a first data store associated with said bastion host and configured to store a set of key-password pairs;

a portable storage device;

a second data store associated with said portable storage device and configured to store passwords represented in said key-password pairs;

a user operable initialization mechanism that interfaces with said first and second data stores, said initialization mechanism generating and storing said key-password pairs in said first data store and generating and storing said passwords in said second data store;

an authentication mechanism having a first component associated with said bastion host and having a second component associated with said client computer;

said first component being configured to communicate a key associated with one of said key-password pairs to said second component;

said second component being configured to access said second data store and retrieve at least one password represented in said key-password pair;

said second component being further configured to communicate said at least one password to said first component based on input from the user and based on said key communicated from said first component.

2. The system of claim 1 further comprising key management system that encrypts and stores said passwords in said second data store.

3. The system of claim 1 wherein said passwords stored in said second data store are encrypted and said second component is configured to decrypt and communicate said at least one password to said first component.

4. The system of claim 1 wherein said portable storage device is a non-volatile memory device.

5. The system of claim 1 wherein said portable storage device is an optical disk.

6. The system of claim 1 further comprising screening router system that blocks interaction with said trusted computer network.

7. The system of claim 6 further comprising proxy system that integrates with said screening router to permit interaction with said trusted computer network under control of said authentication mechanism.

8. The system of claim 1 further comprising session management system that restricts interaction with said trusted computer network to an authenticated active session.

9. The system of claim 1 further comprising session management system that restricts interaction with said trusted computer network to predetermined time duration.

10. The system of claim 1 further comprising a plug-in module stored on said portable storage device and accessible to said client computer to provide said client computer with instructions in implementing said second component of said authentication mechanism.

11. A method of authenticating interaction with a trusted computer network located behind a bastion host, comprising:

defining a secure database protected by said bastion host;

providing a portable storage device;

providing a user-operable recording mechanism protected by said bastion host by which said user stores first information in said secure database and second information in said portable storage device;

said first and second information representing components of an encryption key system from which at least one password is generated;

installing said portable storage device at a client computer and establishing communication between said bastion host and said client computer;

using said first and second information at said client computer to generate said password and communicating said password to said bastion host;

evaluating said password at said bastion host and effecting authentication based on correspondence of said password to information stored in said secure database.

12. The method of claim 11 further comprising providing said portable storage device with a protected area and storing at least a portion of said second information within said protected area.

13. The method of claim 11 wherein said user step of storing second information includes supplying a secret PIN number and subsequently using said PIN number in generating said password.

14. The method of claim 11 comprising providing said portable storage device with a protected area and storing a secret session key within said protected area, said session key being used to encrypt a user-supplied PIN number prior to use.

15. The method of claim 11 further comprising establishing an active session after said step of effecting authentication, and limiting said active session to a predetermined time duration.

16. A computer network authentication signal embodied in a carrier wave, comprising:

an index value representing one of a plurality of one-time passwords;

a key value associated with said index value and corresponding to said one of said plurality of one-time passwords.

17. A secure network communication system, comprising:

a screening router;

an authentication system that authenticates a remote client communicating through said screening router;

a bastion host having web proxy system in communication with said screening router;

active session middleware associated with said bastion host that associates an active session with said remote client upon authentication by said authentication system ;

said web proxy system being configured to perform URL verification and URL modification based on information received from said active session middleware and said authentication system.

18. The system of claim 17 wherein said authentication system includes a portable storage device that supplies one-time passwords to said remote client.

19. The system of claim 17 wherein said web proxy system performs URL modification bi-directionally and operates upon URLs issued both to and from said remote client.

20. The system of claim 17 wherein said web proxy system further includes a template page database that stores at least one log-in page that integrates with said authentication system.

21. The system of claim 17 wherein said authentication system is associated with a gateway and wherein said includes a secure database for storing information used by to authenticate said remote client.

22. The system of claim 17 wherein said active session middleware includes session timer that terminates said active session after a predetermined time.

23. The system of claim 17 wherein said authentication system employs a portable storage device having a protected area that stores a session key used during the authentication process to protect information provided by a user operating said remote client.